REMARKS/ARGUMENTS

Claims 1-16, 18-20 and 22-24 are pending in this application. By this Amendment, claims 7-12 are amended, and claim 21 is cancelled without prejudice or disclaimer. Support for the claims can be found throughout the specification, including the original claims and the drawings. Withdrawal of the rejections in view of the above amendments and the following remarks is respectfully requested.

I. Allowable Subject Matter

It is noted that claim 16 is not rejected over art in the Office Action. It is therefore assumed, for purposes of this reply, that claim 16 defines patentable subject matter.

II. Rejection under 35 U.S.C. §112, Second Paragraph

The Office Action rejects claim 12 under 35 U.S.C. §112, second paragraph. It is respectfully submitted that the amendment to claim 12 is responsive to the Examiner's comments, and that claim 12 meets the requirements of 35 U.S.C. §112, second paragraph. Accordingly, the rejection should be withdrawn.

III. Rejection under 35 U.S.C. §103(a)

The Office Action rejects claims 1, 2, 4, 5, 7, 9, 10 and 21 under 35 U.S.C. §103(a) over U.S. Patent No. 6,088,451 to He in view of U.S. Patent No. 5,862,339 to Bonnaure et al. (hereinafter "Bonnaure"). Claim 21 has been cancelled. This rejection, in so far as it applies to the remaining claims, is respectfully traversed.

Independent claim 1 is directed to a method for accessing the Internet using an Internet

TV system. Independent claim 1 recites transmitting a message from the Internet TV to the server requesting authentication for use of information during a current session, transmitting a message from the server requesting an authentication number from the Internet TV, transmitting the requested authentication number from the Internet TV to the server if the authentication number is available, checking a validity of the transmitted authentication number, and providing information to the Internet TV for the current session if it is determined that the authentication number is valid. Independent claim 1 then recites requesting a new authentication number from the server if the authentication number is not available, registering a user in accordance with information collected by the server, receiving a new authentication number from the server, and providing information to the Internet TV for use during the current session, and storing the new authentication number in a memory device of the Internet TV for use during a later session. Independent claim 7 recites similar features in varying scope. He neither discloses nor suggests the features of independent claims 1 and 7, or the respective claimed combinations of features.

He discloses a security system that controls access to individual network elements 102 using a network security server (NSS) 208, including a registration database 210, an authentication server 202, a credential server 204, and a network element access server (NEAS) 206. As shown in Figure 5 of He, a user registers with a registration database 210 (S404), the authentication server 202 validates the user (S406), and the credential server 204 checks precision of the user's credentials (S408). The NEAS 206 then screens the now validated and credentialed user against element access lists to determine which of the network elements 102

the user is allowed to access (S410), and information flows between the network element 102 and the user (S412) as security auditing is performed (S414).

The login and access request procedures are shown in more detail in Figures 6 and 7 of He. To log in, the user enters an ID and password (S602), and the NSS 208 determines if the ID and password are authentic (S604). Once authenticated, the NEAS 206 searches the database 210 and constructs an access list for the particular user (S608), and the NSS 208 issues a general ticket and the access list to the user (S610, S612). The general ticket allows the user access to the particular network elements 102 in the list compiled by the NEAS 206.

To request access to a particular network element 102 on the list, the user selects the element 102 (S702), and this request is sent to the NSS 208 (S704), which verifies the general ticket and issues a session ticket and a session encryption key (S706) that allow the user to exchange information with the selected element 102 during that session (S708). The user element 102 encrypts and sends data to the selected network element using the session key (S802, S804), and the network element decrypts the session ticket for validation (S806, S808). Once validated, the network element decrypts the received data and acts on the user's request (S812, S814).

Once the user has completed the desired data exchange with the selected network element 102, and has logged out, or the session has timed out, all the tickets that have been issued to the user (the general ticket, the session ticket, and the session encryption key) are destroyed. Thus, if the user wishes to access one of the network elements 102 in a later session

(either the previously accessed element 102 or a different element 102), the user must re-log on to the user element as described above to obtain a new general ticket (see column 28, lines 34-41 of He). He neither discloses nor suggests that any of the issued tickets (compared in the Office Action to the claimed authentication number) are stored in a memory device for use during a later session, as recited in independent claims 1 and 7.

Further, Bonnaure is merely cited in the Office Action as allegedly teaching an Internet TV in Figure 5, and thus fails to overcome the deficiencies of He. Further, the system shown in Figure 5 of Bonnaure shows an ISDN modem connected to a TV. See, for example, column 3, line 66 – column 4, line 3 of Bonnaure, which states that the elements of Bonnaure's system are applied to a standard television set that uses standard telephone lines and/or other residential communication networks as a transport medium. The TV shown in Bonnaure's figures is simply being used as a monitor, and is not, by itself, an Internet TV in which a function of accessing the Internet and a function of receiving a TV broadcast are combined, as recited in independent claim 1.

Accordingly, it is respectfully submitted that independent claims 1 and 7 are allowable over the applied combination, and thus the rejection of independent claims 1 and 7 under 35 U.S.C. §103(a) over He and Bonnaure should be withdrawn. Dependent claims 2, 4, 5, 9 and 10 are allowable at least for the reasons set forth above with respect to independent claims 1 and 7, from which they respectively depend, as well as for their added features.

The Office Action rejects claims 1-4, 7-10, 14 and 20-24 under 35 U.S.C. §103(a) over Bonnaure. Claim 21 has been cancelled. This rejection, in so far as it applies to the remaining claims, is respectfully traversed.

The features of independent claims 1 and 7 are set forth above. As also set forth above, Bonnaure neither discloses nor suggests each of the features of independent claims 1 and 7, or the respective claimed combinations of features. Further, it would not have been obvious to modify the system disclosed by Bonnaure as suggested in the Office Action.

Bonnaure discloses a central routing device that is coupled to a standard residential television set to route access requests for internet access amongst a variety of providers. As shown in Figures 6-7 of Bonnaure, a plurality of WebTV clients 610 are connected to a WebTV server 620 through a point of presence (POP) node 710 and/or a network 612 (such as the Internet). Each client 610 is essentially like a set top box that uses the standard TV to which it is connected as a display monitor for data that is received through the client 610. Each client 610 may include a client box ID 842, an encryption key storage area 844, and a network address storage area 846, and may communicate with the server 620 through a network interface 840 and a communication channel 852.

Automatic number identification (ANI) may be used to identify each client 610 as access is requested (see column 5, lines 41-65 of Bonnaure). The storage areas 844 and 846 may be used to store other types of information used during authentication and encryption processes. However, these storage areas 844 and 846 are part of the WebTV client set top box 610.

Bonnaure neither discloses nor suggests an Internet TV as specifically recited in independent claims 1 and 7. Thus, Bonnaure necessarily neither discloses nor suggests that authentication numbers are stored in a memory device of such an Internet TV, let alone for use during a later session, as recited in independent claims 1 and 7.

Further, it would not have been obvious to modify Bonnaure's system to use an Internet TV instead of the disclosed standard TV and interface device. Bonnaure clearly discloses that an interface device used with a standard TV and standard telephone lines has been selected so that the system may be widely implemented without requiring replacement of existing TVs to provide for access to the WebTV server 620. Rather, it is respectfully submitted that Bonnaure teaches away from such a modification, which would increase cost and complexity and make wide implementation more difficult without replacement of significant amounts of equipment in users' homes.

Accordingly, it is respectfully submitted that independent claims 1 and 7 are allowable over Bonnaure, and thus the rejection of independent claims 1 and 7 under 35 U.S.C. §103(a) over Bonnaure should be withdrawn. Dependent claims 2-4, 8-10, 14, 20 and 22-24 are allowable at least for the reasons set forth above with respect to independent claims 1 and 7, from which they respectively depend, as well as for their added features.

The Office Action rejects claims 5, 6, 11-13, 18 and 19 under 35 U.S.C. §103(a) over Bonnaure in view of U.S. Patent No. 6,449,651 to Dorfman et al. (hereinafter "Dorfman"). The

Office Action also rejects claim 15 under 35 U.S.C. §103(a) over Bonnaure in view of U.S. Patent No. 6,785,716 to Nobakht. These rejections are respectfully traversed.

Dependent claims 5, 6, 11-13, 15, 18 and 19 are allowable over Bonnaure at least for the reasons set forth above with respect to independent claims 1 and 7, from which they respectively depend, as well as for their added features. Further, Dorfman is merely cited as allegedly teaching examination of encryption keys for validity, and Nobakht is merely cited as allegedly teaching transmitting a message indicating that a user fee has not been paid. Thus, Dorfman and Nobakht each fails to overcome the deficiencies of Bonnaure. Accordingly, it is respectfully submitted that claims 5, 6, 11-13, 15, 18 and 19 are allowable over the respective applied combinations, and thus the rejections should be withdrawn.

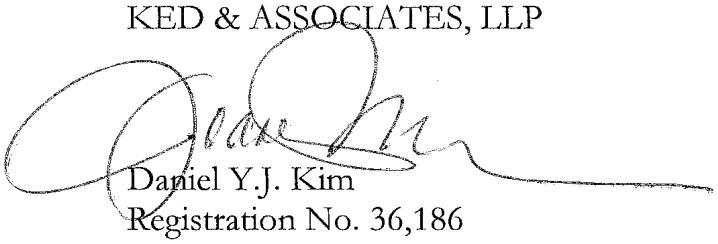
IV. Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that the application is in condition for allowance. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the **Joanna K. Mason**, at the telephone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this,

concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
KED & ASSOCIATES, LLP



Daniel Y.J. Kim
Registration No. 36,186
Joanna K. Mason
Registration No. 56,408

P.O. Box 221200
Chantilly, Virginia 20153-1200
(703) 766-3777 DYK:JKM:lhd
Date: December 10, 2007
\\Fk4\Documents\2000\2000-236\135810.doc
Please direct all correspondence to Customer Number 34610